TTC仕様書
Technical Specification

# TS-M2M-0037v4.0.2

# IoT 公共警報サービスへの適用

# IoT Public Warning Service Enablement

2023 年 3 月 17 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TS-M2M-0037v4.0.2

IoT 公共警報サービスへの適用　[IoT Public Warning Service Enablement]

＜参考＞ [Remarks]

１．英文記述の適用レベル [Application level of English description]

適用レベル [Application level]：E2

本標準の本文、付属資料および付録の文章および図に英文記述を含んでいる。

[English description is included in the text and figures of main body, annexes and appendices.]

２．国際勧告等の関連 [Relationship with international recommendations and standards]

本標準は、oneM2M で承認された Technical Specification TS-0037-V4.0.2 に準拠している。

[This standard is standardized based on the Technical Specification TS-0037-V4.0.2 approved by oneM2M.]

３．上記国際勧告等に対する追加項目等 [Departures from international recommendations]

原標準に対する変更項目 [Changes to original standard]

原標準が参照する標準のうち、TTC 標準に置き換える項目。[Standards referred to in the original standard, which are replaced by TTC standards.]

原標準が参照する標準のうち、それらに準拠した TTC 標準等が制定されている場合は自動的に最新版 TTC 標準等に置き換え参照するものとする。 [Standards referred to in the original standard should be replaced by derived TTC standards.]

４．工業所有権 [IPR]

本標準に関わる「工業所有権等の実施の権利に係る確認書」の提出状況は、ＴＴＣホームページによる。

[Status of “Confirmation of IPR Licensing Condition” submitted is provided in the TTC web site.]

５．作成専門委員会 [Working Group]

oneM2M 専門委員会 [oneM2M Working Group]

# ONEM2M TECHNICAL SPECIFICATION

| | |
|---|---|
| Document Number | TS-0037-V-4.0.2 |
| Document Name: | IoT Public Warning Service Enablement |
| Date: | 2022-10-18 |
| Abstract: | This technical specification specifies the information model of the public warning service, and defines the resource mapping rule for the information model of the public warning. |

'Template Version: January 2019 (do not modify)

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

# Contents

# 1 Scope

The present document specifies the unified information model of the public warning service and defines the resource mapping rule for the information model of the public warning service over oneM2M system. The information model of the public warning service described in this document is applicable not only for an emergency alerting that authorities send the public but also for warnings that used to be distributed to IoT devices in commercial services.

NOTE: The SDT definitions of Public Safety Domain information model will be maintained in TS-0023 in Release 4 and future releases.

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[1] oneM2M TS-0011: "Common Terminology".

[2] oneM2M TS-0023: "SDT based Information Model & Mapping for Vertical Industries".

[3] Recommendation ITU-T X.1303 bis: "Common alerting protocol (CAP 1.2)".

NOTE: Available at https://www.itu.int/rec/T-REC-X.1303bis-201403-I.

[4] Smart Device Template.

NOTE: Available at https://git.onem2m.org/MAS/SDT.

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.2] 3GPP TS 22.268: "Public Warning System (PWS) requirements (Release 16)".

[i.3] IETF RFC 3066: "Tags for the Identification of Languages".

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc3066.

[i.4] World Geodetic System 1984.

NOTE: Available at https://earth-info.nga.mil/php/download.php?file=coord-wgs84.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

Void.

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| ADN | Application Dedicated Node |
| ASN | Application Service Node |
| CAP | Common Alerting Protocol |
| CBRNE | Chemical, Biological, Radiological, Nuclear or high-yield Explosive |
| HTML | Hyper Text Markup Language |
| IETF | Internet Engineering Task Force |
| ITU-T | International Telecommunication Union - Telecommunication |
| JSON | JavaScript Object Notation |
| MN | Middle Node |
| PDT | Pacific Daylight Time |
| PWS | Public Warning System |
| RFC | Request For Comments |
| RW | Read / Write |
| SDT | Smart Device Template |
| SHA | Secure Hash Algorithm |
| SP | Service Provider |
| TS | Technical Specification |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition |

# 4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

# 5 Information Model of Public Warning Service

## 5.1 Background

### 5.1.1 Public Warning Service for Things

Public warning service enables authorities in charge of public safety to send an emergency alert to things in order to make things take a proper action to reduce unexpected damages from an emergency when receiving an emergency alert.

Public warning messages for things include information related to an emergency event such as:

- Geographic targeting area where an emergency event happens.
- Detailed information to provide how to take actions when receiving a public warning message with things.
- Effective period for a valid public warning message.
- Relevant information that is useful for things to take best-effort options to reduce the risk or avoid the emergency.

## 5.1.2 Common Alerting Protocol (CAP)

The CAP is widely used to specify the information model applied for systems of authorities in charge of initiating a public warning message. Figure 5.1.2-1 shows the CAP document object model describing the structure of CAP message and Annex B describe the classification of CAP-based information that is interpretable by things in CAP 1.2 specification [3]. The CAP based information needs to be transformed into oneM2M based information in order to make things understand an emergency event notified from authorities and take a proper action.

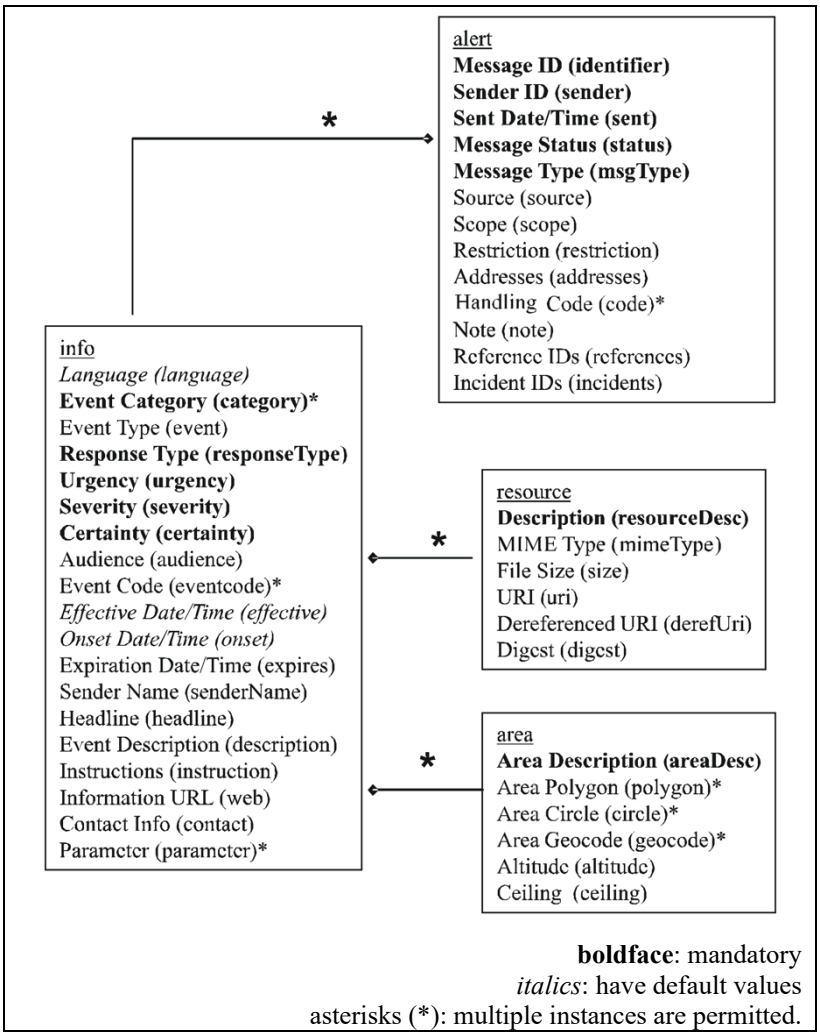


**Figure 5.1.2-1: CAP document object model (source: Recommendation ITU-T X.1303 bis [3])**

## 5.1.3 SDT based information model

The information model of public warning service is specified by SDT schema [4].

## 5.1.4 Possible architecture for oneM2M based public warning service

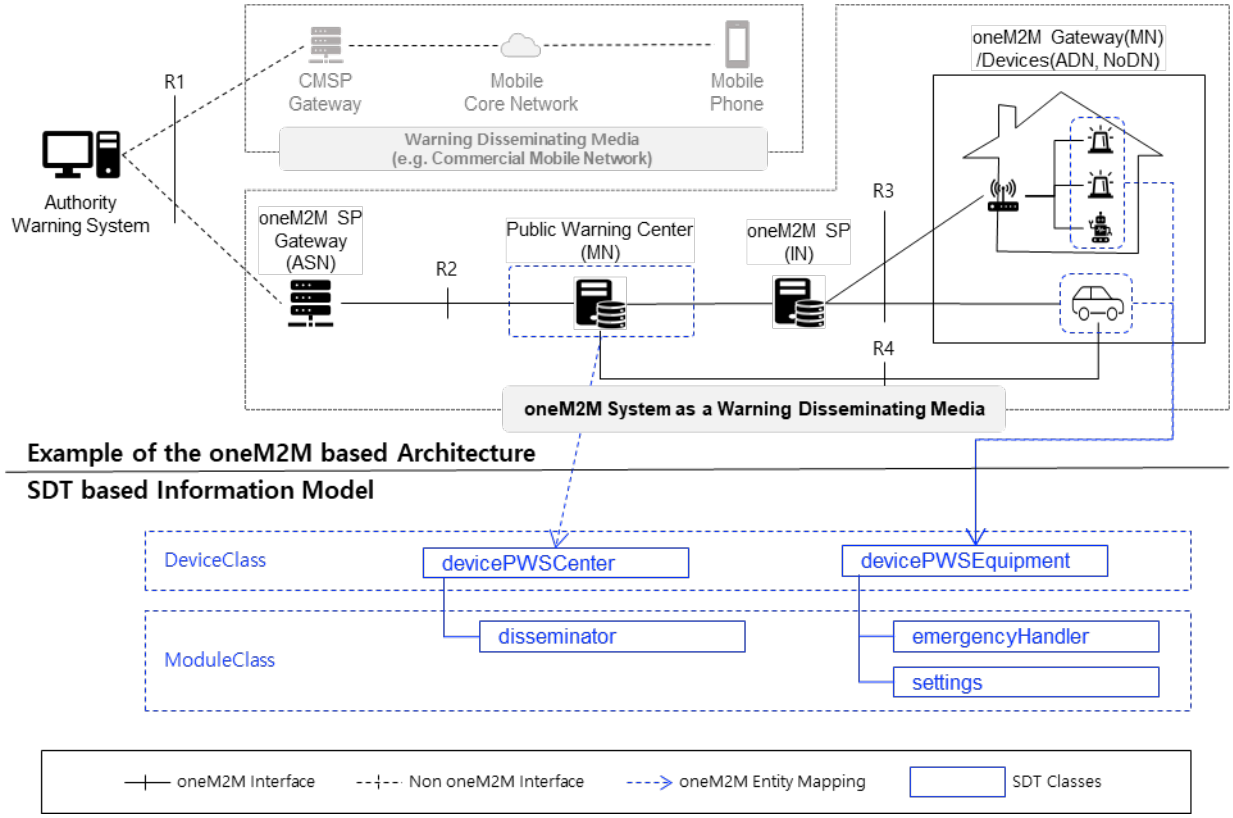


**Figure 5.1.4-1: Possible architecture and SDT mapping**

Figure 5.1.4-1 describes the example of the oneM2M based architecture for public warning service and how MN (public warning center) and devices (ADN) are defined as SDT based information model.

The example of the oneM2M based architecture consists of following functional entities:

- Authority Warning System is the system used by authorities who issue an alert. The CAP based message initiated by Authority Warning System is transmitted to oneM2M SP Gateway but also other warning dissemination media via R1 interface. The interface between Authority Warning System and oneM2M SP Gateway is out of scope of oneM2M specifications.
- oneM2M SP (Service Provider) Gateway (ASN) enables oneM2M Service Provider to interwork with external systems. When the Authority Warning System as an external system issues CAP based information to be disseminated via R1 interface, the oneM2M SP Gateway forwards that CAP based information to the Public Warning Center.
- Public Warning Center (MN) is to transform CAP based information received from oneM2M SP Gateway into oneM2M based information that is interpretable by things. In addition, Public Warning Center (MN) identifies targeted things that need to receive the public warning message issued by Authority Warning System.
- OneM2M Devices (ADN, NoDN) take an action specified in normal mode before receiving a public warning message but change into an emergency mode as receiving a public warning message in order to take an emergency action.

## 5.2 Void

## 5.3 ModuleClasses

### 5.3.1 disseminator

This ModuleClass provides the capability of creating oneM2M based information from CAP based information received from oneM2M SP Gateway (ASN) and of controlling the change of received public warning messages such as updating oneM2M based information and canceling the dissemination of oneM2M based information.

**Table 5.3.1-1: Actions of disseminator ModuleClass**

| Return Type | Name | Argument | Optional | Documentation |
|---|---|---|---|---|
| result: xs:string | cancel | warningIdentifier: xs:string | true | cancel previously requested warning |

**Table 5.3.1-2: DataPoints of disseminator ModuleClass**

| Name | Type | R/W | Optional | Unit | Documentation |
|---|---|---|---|---|---|
| identifier | xs:string | RW | false | | The identifier of the warning message that uniquely identifying this message. |
| sender | xs:string | RW | false | | The identifier of the originator of this alert message. |
| sent | xs:dateTime | RW | false | | The time and date of the origination of this alert message. |
| status | hd:enumAlertStatus | RW | false | | The code to represent the appropriate handling of the alert message receiver. The value of this DataPoint is specified the CAP 1.2 specification [3] (see clause 5.5.2). |
| msgType | hd:enumAlertMsgType | RW | false | | The code to represent the nature of the alert message. The value of this DataPoint is specified the CAP 1.2 specification [3] (see clause 5.5.3). |
| references | list of xs:string | RW | true | | The list of identifiers for earlier message(s) referenced by this alert message. |
| urgency | hd:enumUrgency | RW | false | | The code representing the urgency of the subject event of the alert message (see clause 5.5.4). |
| severity | hd:enumSeverty | RW | false | | The code representing the severity of the subject event of the alert message (see clause 5.5.5). |
| certainty | hd:enumCertainty | RW | false | | The code representing the certainty of the subject event of the alert message (see clause 5.5.6). |
| eventCodes | list of xs:string | RW | false | | The definitions of system-specific codes identifying the event type of the alert message. A code definition consists of valueName and |

| Name | Type | R/W | Optional | Unit | Documentation |
|---|---|---|---|---|---|
| | | | | | value pair separated by colon. |
| effective | xs:dateTime | RW | true | | The effective time of the information of the alert message. |
| onset | xs:dateTime | RW | true | | The expected time of the beginning of the subject event of the alert message. |
| expires | xs:dateTime | RW | true | | The expiry time of the information of the alert message. |
| areaLatitude | xs:float | RW | true | degrees | The latitude of the affected area location. |
| areaLongitude | xs:float | RW | true | degrees | The longitude of the affected area location. |
| areaRadius | xs:float | RW | true | meters | The radius of the affected area location. |
| repetitionPeriod | xs:integer | RW | false | seconds | This specifies the repetition period for the warning message. The value of this DataPoint indicates the period of time in seconds after which re-send of the warning message should be repeated. |
| repetitionCount | xs:integer | RW | false | | This specifies the number of times the warning message is to be sent. |

## 5.3.2 emergencyHandler

This ModuleClass provides the capability of triggering things to change into an emergency mode and of enabling things to identify whether an event described in oneM2M based information that is received from Public Warning Center (MN) is relevant to things. If any change happens in received warning messages such as updating oneM2M based information and cancelling the dissemination of oneM2M based information of previously received public warning messages, this ModuleClass updates oneM2M based information corresponding to those received public warning messages to control behaviour of things.

**Table 5.3.2-1: DataPoints of emergencyHandler ModuleClass**

| Name | Type | R/W | Optional | Unit | Documentation |
|---|---|---|---|---|---|
| emergencyMode | xs:boolean | RW | false | | This specifies the emergency mode of target device. "True" means the device is working in emergency mode. "False" means the device is working in normal model |
| identifier | xs:string | RW | false | | The identifier of the warning message that uniquely identifying this message. |
| sender | xs:string | RW | false | | The identifier of the originator of this alert message. |
| sent | xs:dateTime | RW | false | | The time and date of the origination of this alert message. |
| status | hd:enumAlertStatus | RW | false | | The code to represent the appropriate handling of the alert message receiver. The value of this DataPoint is specified the CAP 1.2 specification [3] (see clause 5.5.2). |

| Name | Type | R/W | Optional | Unit | Documentation |
|---|---|---|---|---|---|
| msgType | hd:enumAlertMsgType | RW | false | | The code to represent the nature of the alert message. The value of this DataPoint is specified the CAP 1.2 specification [3] (see clause 5.5.3). |
| references | list of xs:string | RW | false | | The list of identifiers for earlier message(s) referenced by this alert message. |
| urgency | hd:enumUrgency | RW | false | | The code representing the urgency of the subject event of the alert message (see clause 5.5.4). |
| severity | hd:enumSeverty | RW | false | | The code representing the severity of the subject event of the alert message (see clause 5.5.5). |
| certainty | hd:enumCertainty | RW | false | | The code representing the certainty of the subject event of the alert message (see clause 5.5.6). |
| eventCodes | list of xs:string | RW | false | | The definitions of system-specific codes identifying the event type of the alert message. A code definition consists of valueName and value pair separated by colon. |
| effective | xs:dateTime | RW | true | | The effective time of the information of the alert message. |
| onset | xs:dateTime | RW | true | | The expected time of the beginning of the subject event of the alert message. |
| expires | xs:dateTime | RW | true | | The expiry time of the information of the alert message. |
| areaLatitude | xs:float | RW | true | deg | The latitude of the affected area location. |
| areaLongitude | xs:float | RW | true | deg | The longitude of the affected area location. |
| areaRadius | xs:float | RW | true | m | The radius of the affected area location. |

## 5.3.3 settings

This ModuleClass provides the capability of selecting the option that allows things to decide to take action as receiving oneM2M based information of public warning messages.

**Table 5.3.3-1: DataPoints of settings ModuleClass**

| Name | Type | R/W | Optional | Unit | Documentation |
|---|---|---|---|---|---|
| optoutStatus | xs:boolean | RW | false | | This specifies the opt-out state for the device. The value of this DataPoint specifies opt-out state. True means that this device does not want to response when a warning has been triggered. |
| NOTE: Opt-out is refer to 3GPP TS 22.268 [i.2] Public Warning System (PWS) requirements specification. | | | | | |

## 5.4 Device models

### 5.4.1 devicePWSCenter

**Table 5.4.1-1: Modules of devicePWSEquipment Device**

| Module Instance Name | Module Class Name | Multiplicity | Description |
|---|---|---|---|
| disseminator | disseminator | 1 | See clause 5.3.1 |

### 5.4.2 devicePWSEquipment

**Table 5.4.2-1: Modules of devicePWSEquipment Device**

| Module Instance Name | Module Class Name | Multiplicity | Description |
|---|---|---|---|
| emergencyHandler | emergencyHandler | 1 | See clause 5.3.2 |
| settings | settings | 1 | See clause 5.3.3 |

## 5.5 Enumeration type definitions

### 5.5.1 Introduction

This clause defines the enumeration type of the domain for public warning service. The "pws" namespace qualifier is used to indicate the terms of the domain for public warning service.

### 5.5.2 hd:enumAlertStatus

The enumeration type, hd:enumAlertStatus, enables things to identify the alert status that describes whether a received public warning message as oneM2M based information is an actual alert issued by authorities or an alert for testing the public warning service over oneM2M system.

**Table 5.5.2-1: Interpretation of hd:enumAlertStatus**

| Value | Interpretation | Note |
|---|---|---|
| 1 | Actual | Actionable by all targeted recipients |
| 2 | Exercise | Actionable only by designated exercise participants |
| 3 | System | For messages that support alert network internal functions |
| 4 | Test | Technical testing only, all recipients disregard |
| 5 | Draft | A preliminary template or draft, not actionable in its current form |
| NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [3]. | | |

### 5.5.3 hd:enumAlertMsgType

The enumeration type, hd:enumAlertMsgType, describes the message type of oneM2M based information transformed from CAP based information issued by authorities.

**Table 5.5.3-1: Interpretation of hd:enumAlertMsgType**

| Value | Interpretation | Note |
|---|---|---|
| 1 | Alert | Initial information requiring attention by targeted recipients |
| 2 | Update | Updates and supersedes the earlier message(s) |
| 3 | Cancel | Cancels the earlier message(s) |
| NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [3]. | | |

### 5.5.4 hd:enumUrgency

The enumeration type, hd:enumUrgency, describes the urgency of the event defined in oneM2M based information transformed from CAP based information issued by authorities.

**Table 5.5.4-1: Interpretation of hd:enumUrgency**

| Value | Interpretation | Note |
|---|---|---|
| 1 | Immediate | Responsive action should be taken immediately |
| 2 | Expected | Responsive action should be taken soon (within next hour) |
| 3 | Future | Responsive action should be taken in the near future |
| 4 | Past | Responsive action is no longer required |
| 5 | Unknown | Urgency not known |
| NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [3]. | | |

### 5.5.5 hd:enumSeverity

The enumeration type, hd:enumSeverity, describes the severity of the event defined in oneM2M based information transformed from CAP based information issued by authorities.

**Table 5.5.5-1: Interpretation of hd:enumSeverity**

| Value | Interpretation | Note |
|---|---|---|
| 1 | Extreme | Extraordinary threat to life or property |
| 2 | Severe | Significant threat to life or property |
| 3 | Moderate | Possible threat to life or property |
| 4 | Minor | Minimal to no known threat to life or property |
| 5 | Unknown | Severity unknown |
| NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [3]. | | |

### 5.5.6 hd:enumCertainty

The enumeration type, hd:enumCertainty, describes the certainty of the event defined in oneM2M based information transformed from CAP based information issued by authorities.

**Table 5.5.6-1: Interpretation of hd:enumCertainty**

| Value | Interpretation | Note |
|---|---|---|
| 1 | Observed | Determined to have occurred or to be ongoing |
| 2 | Likely | Likely (p > ~50 %) |
| 3 | Possible | Possible but not likely (p ≤ ~50 %) |
| 4 | Unlikely | Not expected to occur (p ~ 0) |
| 5 | Unknown | Certainty unknown |
| NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [3]. | | |

# 6 Resource Mapping

## 6.1 Resource Mapping Rules

The resource mapping rule of the information model of public warning service is defined according to the clause 6.2 of oneM2M TS-0023 [2].

# 6.2 Short names

## 6.2.1 Introduction

XML and JSON representations require the explicit encoding of the names of resource attributes, (in the case of XML) and resource types. Whenever a protocol binding transfers such a name over a oneM2M reference point, it shall use a shortened form of that name. Short names enable payload reduction on involved telecommunication interfaces.

The mapping between the full names and their shortened form is given in the clauses that follow.

## 6.2.2 Resource types

In protocol bindings, resource type names for device models shall be translated into short names of Table 6.2.2-1.

**Table 6.2.2-1: Specialization type short names (Devices)**

| Resource Type Name | Short Name |
|---|---|
| devicePWSCenter | ***dPWSC*** |
| devicePWSEquipment | ***dPWSE*** |

In protocol bindings, resource type names for module classes shall be translated into short names of Table 6.2.2-2.

**Table 6.2.2-2: Specialization type short names (ModuleClasses and Module Instances)**

| Resource Type Name | Short Name |
|---|---|
| disseminator | ***dissr*** |
| emergencyHandler | ***emeHr*** |
| settings | ***setts*** |

In protocol bindings, resource type names for actions shall be translated into short names of Table 6.2.2-3.

**Table 6.2.2-3: Specialization type short names (Actions)**

| Resource Type Name | Short Name |
|---|---|
| cancel | ***cancl*** |

## 6.2.3 Resource attributes for properties and data points

In protocol bindings resource attributes names for properties of module classes shall be translated into short names of Table 6.2.3-1.

**Table 6.2.3-1: Resource attribute short names (ModuleClass properties)**

| Attribute Name | Occurs in | Short Name |
|---|---|---|
| areaLatitude | disseminator, emergencyHandler | ***areLe*** |
| areaLongitude | disseminator, emergencyHandler | ***areL0*** |
| areaRadius | disseminator, emergencyHandler | ***areRs*** |
| certainty | disseminator, emergencyHandler | ***certy*** |
| effective | disseminator, emergencyHandler | ***effee*** |
| emergencyMode | emergencyHandler | ***emeMe*** |
| eventCodes | disseminator, emergencyHandler | ***eveCs*** |
| expires | disseminator, emergencyHandler | ***expis*** |
| identifier | disseminator, emergencyHandler | ***idenr*** |
| msgType | disseminator, emergencyHandler | ***msgTe*** |
| onset | disseminator, emergencyHandler | ***onset*** |
| optoutStatus | settings | ***optSs*** |
| references | disseminator, emergencyHandler | ***refes*** |
| repetitionPeriod | disseminator | ***repPd*** |
| repetitionCount | disseminator | ***repCt*** |

| Attribute Name | Occurs in | Short Name |
|---|---|---|
| sender | disseminator, emergencyHandler | ***sendr*** |
| sent | disseminator, emergencyHandler | ***sent*** |
| severity | disseminator, emergencyHandler | ***sevey*** |
| status | disseminator, emergencyHandler | ***stats*** |
| urgency | disseminator | ***urgey*** |

# 6.3 containerDefinition values

## 6.3.1 Introduction

The rules for constructing containerDefinition values and their usage principles are defined in TS-0023 [2].

## 6.3.2 Device models

The containerDefinition attributes of the specialization for device models of Public Safety Domain are defined as follow.

**Table 6.3.2-1: Definition of containerDefinition attribute for public warning service device models**

| Name | containerDefinition | Description |
|---|---|---|
| devicePWSCenter | org.onem2m.publicsafety.device.devicePWSCenter | See clause 5.4.1 |
| devicePWSEquipment | org.onem2m.publicsafety.device.devicePWSEquipment | See clause 5.4.2 |

## 6.3.3 ModuleClasses

The containerDefinition attributes of the specialization for module classes of Public Safety Domain are defined as follows.

**Table 6.3.3-1: Definition of containerDefinition attribute for public warning service module classes**

| Name | containerDefinition | Description |
|---|---|---|
| disseminator | org.onem2m.publicsafety.moduleclass.disseminator | See clause 5.3.1 |
| emergencyHandler | org.onem2m.publicsafety.moduleclass.emergencyHandler | See clause 5.3.2 |
| settings | org.onem2m.publicsafety.moduleclass.settings | See clause 5.3.3 |

## 6.3.4 Action Models

The containerDefinition attributes of the specialization for action models of Public Safety Domain are defined as follows

**Table 6.3.4-1: Definition of containerDefinition attribute for public warning service action models**

| Module Class | Action | containerDefinition | Description |
|---|---|---|---|
| disseminator | cancel | org.onem2m.publicsafety.action.cancel | See clause 5.3.1 |

# 6.4 XSD definitions

The XSD definitions for Device, ModuleClass and Action are defined according to the clause 6.5 of oneM2M TS-0023 [2].

# Annex A (informative): Warning dissemination using group resource

The oneM2M system supports hierarchical group resources by using sub-group features that are applicable to the dissemination function of a public warning message to multiple devices.

Figure A-1 depicts an example of a hierarchical group structure to disseminate a public warning message to some of targeted areas selectively.

Hierarchical group mechanism is applicable to any multi-level categorization (e.g. type of devices, type of emergency events and severity of warning, etc.).

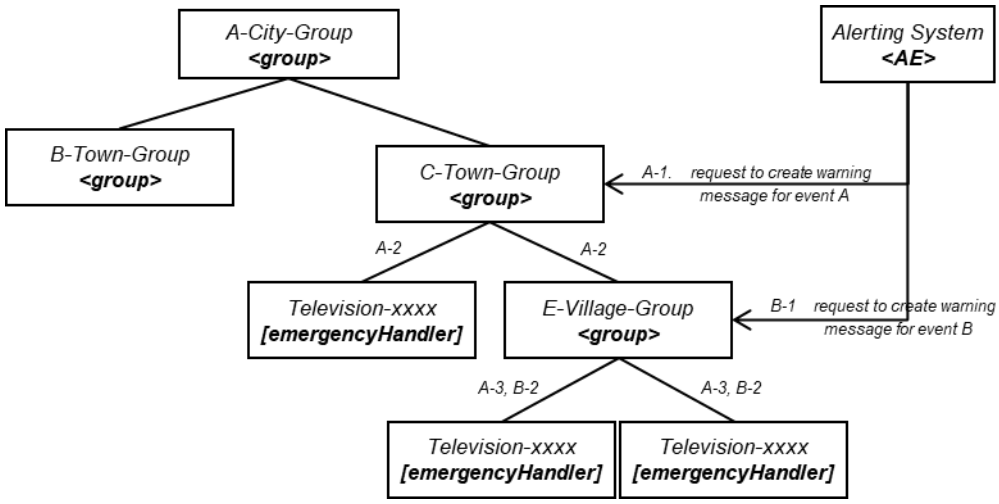


**Figure A-1: Example of <group> resource structure for disseminate warning messages**

- (A-1) request to create a warning message instance to a target <group> resource (e.g. C-Town-Group) to disseminate warning for emergence event (Warning-A).
- (A-2) fan out the requested operation to all members of the group. A member can be a <flexContainer> specialization of [emergencyHandler] (see clause 5.3.2) or a sub-group.
- (A-3) fan out the requested operation repeatedly if fanned out target is a sub-group.
- (A-2, A-3) eventually, all members including members in sub-group can receive the request to create warning message instance for emergency event A.
- (B-1) request to create a warning message instance to a target <group> resource (e.g. C-Town-Group) to disseminate warning for emergence event (Warning-B).
- (B-2) fan out the requested operation to all members of the group. eventually, all member devices of the target <group> resource (e.g. C-Town-Group) receive the request to create warning message instance for emergency event B.

# Annex B (informative): Machine interpretable information of CAP message

## B.1 Machine interpretable information of the *CAP <alert> element*

The <alert> element provides basic information for current public warning message that consists of its purpose, source and status, as well as a unique identifier for the current warning message. Table B.1-1 shows the classification of attributes for CAP <alert> element that is interpretable by things

**Table B.1-1: The classification of attributes for <alert> element**

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| identifier | xs:string | The identifier of the alert message, contains a number or string value that uniquely identifying this message. | Interpretable |
| sender | xs:string | The identifier of the originator of this alert message. This value should be guaranteed by assigner to be unique globally. | Interpretable |
| sent | xs:dateTime | The time and date of the origination of this alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT) | Interpretable |
| status | xs:string | The code to represent the appropriate handling of the alert message receiver. The CAP 1.2 specification [3] restricts code values as below:<br>• "Actual" - Actionable by all targeted recipients<br>• "Exercise" - Actionable only by designated exercise participants; exercise identifier SHOULD appear in <note><br>• "System" - For messages that support alert network internal functions<br>• "Test" - Technical testing only, all recipients disregard<br>• "Draft" -- A preliminary template or draft, not actionable in its current form | Interpretable |
| msgType | xs:string | The code to represent the nature of the alert message. The CAP 1.2 specification restricts code values as below:<br>• "Alert" - Initial information requiring attention by targeted recipients<br>• "Update" - Updates and supersedes the earlier message(s) identified in <references><br>• "Cancel" - Cancels the earlier message(s) identified in <references><br>• "Ack" - Acknowledges receipt and acceptance of the message(s) identified in <references><br>• "Error" - Indicates rejection of the message(s) identified in <references>; explanation should appear in <note> | Interpretable |
| source | xs:string | Not standardized human readable text identifying an operator or a specific device as the source of the alert message. | Not interpretable |
| scope | xs:string | The code to represent the intending scope of distribution for this alert message. The CAP 1.2 specification restricts code values as below:<br>• "Public" - For general dissemination to unrestricted audiences<br>• "Restricted" - For dissemination only to users with a known operational requirement (see <restriction>, below)<br>• "Private" - For dissemination only to specified addresses (see <addresses>, below) | Interpretable |
| restriction | xs:string | Not standardized human readable text to denote the rule for limiting distribution of the restricted alert message. This property appears when "scope" value is "Restricted". | Not interpretable |
| addresses | xs:string (Separated by white space) | The list of addresses of recipients of the alert message. Value of address can be an identifier or an address. This property is required when "scope" value is "Private" and optional when "scope" value is "Public" or "Restricted". | If the value of an address is an identifier, this field would be Machine interpretable |
| code | xs:string | User-defined flag or special code used to handle specially. Multiple code can be presented for an alert message. The format and semantics of the code value are not defined in CAP 1.2 specification. | Interpretable |
| note | xs:string | Not standardized human readable text clarifying the purpose or significant of the alert message when "status" value is "Exercise" and "msgType" value is "Error". | Not interpretable |
| references | xs:string (Separated by white space) | The list of identifiers for earlier message(s) referenced by this alert message. | Interpretable |

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| incidents | xs:string (Separated by white space) | The list of names which are referenced incident(s) of the alert message. | Not interpretable |
| info | xs:complex Type(<info> element) | The container for all component parts of the info sub-element of the alert message.<br>Multiple occurrences are permitted within a single <alert> element to support multiple language or sequence of alert information for an alert message. | n/a (This property is a sub-element described in Table B.2-1) |

# B.2 Machine interpretable information of the CAP <info> element

The <info> element provides both categorical and textual description of the subject emergency event. It may also provide instructions for appropriate response against the received warning message and extra details (e.g. hazard duration, technical parameters, contact information, links to additional media resource, etc.). Table B.2-1 shows the classification of attributes for CAP <info> element that is interpretable by things

**Table B.2-1: The classification of attributes for <info> element**

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| language | xs:language | Contains a IETF RFC 3066 [i.3] code value denoting the language of the info sub-element of the alert message. | Interpretable |
| category | xs:string | The code denoting the category of the alerting event of the alert message. The CAP 1.2 specification [3] restricts code values as below. Multiple category can be presented in an <info> element:<br>• "Geo" - Geophysical (e.g. landslide)<br>• "Met" - Meteorological (e.g. flood)<br>• "Safety" - General emergency and public safety<br>• "Security" - Law enforcement, military, homeland and local/private security<br>• "Rescue" - Rescue and recovery<br>• "Fire" - Fire suppression and rescue<br>• "Health" - Medical and public health<br>• "Env" - Pollution and other environmental<br>• "Transport" - Public and private transportation<br>• "Infra" - Utility, telecommunication, other non-transport infrastructure<br>• "CBRNE" -- Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack<br>• "Other" - Other events | Interpretable |
| event | xs:string | Not standardized human readable text describing the type of the subject event of the alert message | Not interpretable |

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| responseType | xs:string | The code denoting the type of recommended response action for the target audience when the alert message received. The CAP 1.2 specification restricts code values as below. Multiple responseType can be presented in an <info> element:<br>• "Shelter" - Take shelter in place or per <instruction><br>• "Evacuate" - Relocate as instructed in the <instruction><br>• "Prepare" - Make preparations per the <instruction><br>• "Execute" - Execute a pre-planned activity identified in <instruction><br>• "Avoid" - Avoid the subject event as per the <instruction><br>• "Monitor" - Attend to information sources as described in <instruction><br>• "Assess" - Evaluate the information in this message. (This value SHOULD NOT be used in public warning applications.)<br>• "AllClear" - The subject event no longer poses a threat or concern and any follow on action is described in <instruction><br>• "None" - No action recommended | Interpretable |
| urgency | xs:string | The code representing the urgency of the subject event of the alert message. The CAP 1.2 specification restricts code values as below:<br>• "Immediate" - Responsive action SHOULD be taken immediately<br>• "Expected" - Responsive action SHOULD be taken soon (within next hour)<br>• "Future" - Responsive action SHOULD be taken in the near future<br>• "Past" - Responsive action is no longer required<br>• "Unknown" - Urgency not known | Interpretable |
| severity | xs:string | The code representing the severity of the subject event of the alert message. The CAP 1.2 specification restricts code values as below:<br>• "Extreme" - Extraordinary threat to life or property<br>• "Severe" - Significant threat to life or property<br>• "Moderate" - Possible threat to life or property<br>• "Minor" - Minimal to no known threat to life or property<br>• "Unknown" - Severity unknown | Interpretable |
| certainty | xs:string | The code representing the certainty of the subject event of the alert message. The CAP 1.2 specification restricts code values as below:<br>• "Observed" - Determined to have occurred or to be ongoing<br>• "Likely" - Likely (p > ~50 %)<br>• "Possible" - Possible but not likely (p ≤ ~50 %)<br>• "Unlikely" - Not expected to occur (p ~ 0)<br>• "Unknown" - Certainty unknown | Interpretable |
| audience | xs:string | Not standardized human readable text describing the intended audience of the alert message | Not interpretable |
| eventCode | xs:complexType | The definitions of system-specific codes identifying the event type of the alert message. A code definition consists of valueName and value. Multiple eventCode can be presented in an <info> element. | Interpretable |
| effective | xs:dateTime | The effective time of the information of the alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). If this value is not presented, effective time is assumed to be the same time as in "sent" | Interpretable |

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| onset | xs:dateTime | The expected time of the beginning of the subject event of the alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). | Interpretable |
| expires | xs:dateTime | The expiry time of the information of the alert message. This value should be represented in the Date Time format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). If this value is not presented, recipient can set own expiration policy. | Interpretable |
| senderName | xs:string | Not standardized human readable name of the agency or authority issuing this alert message. | Not interpretable |
| headline | xs:string | Not standardized human readable short headline text of the alert message. 160 characters are recommended. | Not interpretable |
| description | xs:string | Not standardized human readable extended description of the hazard or event that occasioned this message. | Not interpretable |
| instruction | xs:string | Not standardized human readable instruction describing recommended action to targeted recipients. | Not interpretable |
| web | xs:anyURI | The hyperlink URI for an HTML page or text resource to provide additional information for the alert message | Interpretable |
| contact | xs:string | Not standardized human readable text describing the contact for follow-up and confirmation of the alert message. | Not interpretable |
| parameter | xs:complex Type | The definitions of system-specific parameter associated with the alert message. A parameter definition consists of valueName and value. Multiple parameters can be presented in an <info> element. | Interpretable |
| resource | xs:complex Type(<resource> element) | The definitions of all component parts of the resource refers to an additional file. This definition to be used to provide multimedia file to recipients. Multiple resource can be presented in an <info> element. | n/a (This property is a sub-element described in Table B.3-1) |
| area | xs:complex Type(<area> element) | The definition of all component parts of the area identifying an affected area. A <info> element may contain one or multiple area definition to identify union of all the included area. | n/a (This property is a sub-element described in Table B.4-1) |

# B.3 Machine interpretable information of the CAP <resource> *element*

The <resource> element provides additional information about subject event in the form of a digital asset such as an image or audio resource link. Table B.3-1 shows the classification of attributes for CAP <resource> element that is interpretable by things

**Table B.3-1: The classification of attributes for <resource> element**

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| resourceDesc | xs:string | Not standardized human readable description of the type and content of a referenced resource file (for example a map or photograph). | Not interpretable |
| mimeType | xs:string | The MIME type, as described in [RFC2046], identifier describing the referenced resource file. | Interpretable |
| size | xs:integer | The approximate size of the resource file in bytes indicating the size of the referenced resource file. | Interpretable |
| uri | xs:anyURI | The hyperlink URL that can be used to retrieve the resource over the Internet. | Interpretable |
| derefUri | xs:string | An alternative to the uri resource hyperlink giving the Base64 encoded content of the resource file. | Interpretable |
| digest | xs:string | The SHA-1 hash value of the resource file for validation. | Interpretable |

# B.4 Machine interpretable information of the CAP <area> *element*

The <area> element describes a geographic area that specifies the target area to which propagate for the related emergency event. Table B.4-1 shows the classification of attributes for CAP <area> element that is interpretable by things

**Table B.4-1: The classification of attributes for <area> element**

| Name | Type | Description | Machine interpretability |
|---|---|---|---|
| areaDesc | xs:string | Not standardized human readable description of the affected area of the alert message. | Not interpretable |
| polygon | xs:string | The space-separated list of coordinate pair defines the polygon that identify the affected area of the alert message. Each coordinate value contains geolocation position value as specified in WGS84 standard [i.4]. Multiple polygons in an <area> element is used to identify union of all polygons. | Interpretable |
| circle | xs:string | The space-separated list of coordinates for a center position and a radius that identify the affected area of the alert message. The first two WGS84 [i.4] geolocation position values represent the center position of the circle, and last value represents the radius delineating in kilometres. Multiple circles in an <area> element is used to identify union of all polygons. | Interpretable |
| geocode | xs:complex Type | The geographic code identifying the affected area of the alert message. A geocode consists of valueName and value. Multiple geocode can be presented in an <area> element. | Interpretable |
| altitude | xs:decimal | The specific or minimum altitude in feet above mean sea level of the affected area of the alert message. | Interpretable |
| ceiling | xs:decimal | The maximum altitude in feet above mean sea level of the affected area of the alert message. | Interpretable |

# History

| Publication history | | |
|---|---|---|
| V1.0.1 | June 2021 | Partners pre-processing done by ***editHelp!***<br>e-mail: mailto:edithelp@etsi.org |
| V4.0.1 | September 2022 | Includes agreed contribution at RDM#55:<br>RDM-2022-0059-TS-0037_Alignment_with_TS-0023<br>RDM-2022-0060-TS-0037_Correction_of_enumeartion_values |
| V4.0.2 | November 2022 | Includes agreed contribution at RDM#56:<br>RDM-2022-0073 Clarification_on_SDT_maintenance |
| | | |
| | | |

| Draft history (to be removed on publication) | | |
|---|---|---|
| V0.0.1 | 2019-12-6 | Skeleton of the TS. |
| V0.1.0 | 2020-10-13 | Includes agreed contribution at RDM#44:<br>RDM-2020-0020R02- TS-00xx Interworking with Public Warning Service System |
| V0.9.0 | 2020-10-22 | Includes agreed contribution at RDM#47:<br>RDM-2020-0079R03- TS-0037 IoT Public Warning Service Enablement |
| V1.0.0 | 2021-4-6 | Includes agreed contribution at RDM#49.1:<br>RDM-2021-0019-Resolve_Editor's_Notes<br>RDM-2021-0020R01-replacement_of_area_datapoint<br>RDM-2021-0021R01-RDM-2021-0021-Editorial_updates |
| | | |